Claims

[c1] A method for verifying an identity of a new-user of a computer system, comprising:

a. receiving at least one identity attribute from the new-user;

b. similarity searching the at least one new-user identity attribute against at least one database of denied-user identity attributes;

c. receiving a similarity search result;

d. determining a positive or negative match between the at least one new-user identity attribute and the denied-user identity attributes;

e. allowing the new-user to access the computer system, where a negative match has been determined; and

f. denying the new-user access to the computer system, where a positive match has been determined.

[c2] The method of claim 1, wherein the at least one new-user identity attribute comprises a new-user profile.

[c3] The method of claim 2, wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles.

[c4] The method of claim 3, wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database.

[c5] The method of claim 1, wherein the step of determining a positive or negative match further comprises comparing the similarity search result to a first match tolerance level.

[c6] The method of claim 5, wherein a positive match comprises a match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that meets or exceeds the first match tolerance level.

[c7] The method of claim 5, wherein a negative match comprises a match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that does not meet or exceed the first match

tolerance level.

[c8] The method of claim 1, further comprising, where a positive match has been determined, verifying the positive match via a secondary review, after the step of determining whether a positive or negative match exists and before the step of denying the new-user access to the computer system.

[c9] The method of claim 8, wherein the step of verifying the positive match further comprises comparing the similarity search result to a second match tolerance level.

[c10] The method of claim 8, further comprising allowing the new-user to access the computer system, where the positive match does not meet or exceed the second match tolerance level.

[c11] The method of claim 8, further comprising denying the new-user access to the computer system, where the positive match meets or exceeds the second match tolerance level.

[c12] The method of claim 1, further comprising, after determining whether a positive or negative match exists, the steps of:
adding the new-user identity to at least one database of valid user identities, where a negative match has been determined; and
adding the new-user identity attributes to the at least one database of denied-user identity attributes, where a positive match has been determined.

[c13] The method of claim 1, wherein the at least one new-user identity attribute is received from at least one component, chosen from a group consisting of Internet web sites, relational databases, data entry systems, and hierarchical databases.

[c14] The method of claim 1, wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes.

[c15] A software program embodied on a computer-readable medium

incorporating the method of claim 1.

[c16] A method for verifying an identity of a new-user of a computer system, comprising:

a. receiving at least one identity attribute from the new-user;

b. similarity searching the at least one identity attribute against at least one database of denied-user identity attributes;

c. receiving a similarity search result;

d. determining a positive or negative match between the at least one new-user identity attribute and the denied-user identity attributes;

e. allowing the new-user to access the computer system and adding the new-user identity to at least one database of valid user identities, where a negative match has been determined;

f. where a positive match has been determined, verifying the positive match via a secondary review;

g. allowing the new-user to access the computer system and adding the new-user identity to at least one database of valid user identities, where the positive match is not verified; and

h. denying the new-user access to the computer system and adding the at least one new-user identity attribute to at least one database of denied-user identity attributes, where the positive match is verified.

[c17] The method of claim 16, wherein the at least one new-user identity attribute comprises a new-user profile.

[c18] The method of claim 17, wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles.

[c19] The method of claim 18, wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database.

[c20] The method of claim 16, wherein the step of determining a positive or negative match further comprises comparing the similarity search result to a

first match tolerance level.

[c21] The method of claim 20, wherein a positive match comprises a match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that meets or exceeds the first match tolerance level.

[c22] The method of claim 20, wherein a negative match comprises a match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that does not meet or exceed the first match tolerance level.

[c23] The method of claim 16, wherein the step of verifying the positive match further comprises comparing the similarity search result to a second match tolerance level.

[c24] The method of claim 1, wherein the at least one new-user identity attribute is received from at least one component, chosen from a group consisting of Internet web sites, relational databases, data entry systems, and hierarchical databases.

[c25] The method of claim 1, wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes.

[c26] A software program embodied on a computer-readable medium incorporating the method of claim 16.

[c27] A system for verifying an identity of a new-user of a computer system, comprising:
a means for receiving at least one identity attribute from the new-user;
at least one database for storing denied-user identity attributes;
at least one database for storing valid user identities;
a means for similarity searching the at least one identity attribute against the at least one database of denied-user attributes;
a means for determining a positive or negative match between the at least

one new-user attribute and the at least one database of denied-user identity attributes;

a means for allowing the new-user to access the computer system, where a negative match has been determined;

a means for denying the new-user access to the computer system, where a positive match has been determined;

a means for adding the new-user identity to the at least one database for storing valid user identities, where a negative match has been determined; and

a means for adding the at least one new-user identity attribute to the at least one database of denied-user attributes, where a negative match has been determined.